Dell DL4300-Gerät
Bereitstellungshandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Copyright © 2015 Dell Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch US-amerikanische und internationale Urheberrechtsgesetze und nach sonstigen Rechten an geistigem Eigentum geschützt. Dell™ und das Dell Logo sind Marken von Dell Inc. in den Vereinigten Staaten und/oder anderen Geltungsbereichen. Alle anderen in diesem Dokument genannten Marken und Handelsbezeichnungen sind möglicherweise Marken der entsprechenden Unternehmen.

2015 - 04

Rev. A00

Inhaltsverzeichnis

1 Einrichten des DL4300-Geräts 5

Einführung 5
Verfügbare Konfigurationen 5
In diesem Dokument verwendete Begriffe 6
Installationsvoraussetzungen 6
Netzwerkanforderungen 6
Empfohlene Netzwerkinfrastruktur 6
Einrichten der Hardware 6
Installation des Systems in einem Rack 7
Einstellen des Konfigurationsschalters für das Speichergehäuse 7
Anschließen des Speichergehäuses an das System 7
Anschließen des Kabelführungsarms (optional) 9
Verkabelung des Systems 9
Einschalten des Systems 9
DL4300-Laufwerkskonfigurationen 10

2 Anfänglicher Software-Setup 11

AppAssure-Systemkonfigurationsassistent 12
Konfiguration der Netzwerkschnittstelle 12
Konfiguration der Host-Namen- und Domain-Einstellungen 13
Konfigurieren der SNMP-Einstellungen 14
Appliance-Schnellselbstwiederherstellung 14
Erstellen von Windows- und RASR-virtuellen Festplatten 14
Erstellen des RASR-USB-Sticks 15
Ausführen von RASR über den RASR-USB-Schlüssel 16
Ausführen von RASR über das interne Dual SD-Modul 17
Speicherbereitstellung 17
Konfiguration von DL4300 unter Verwendung der Fibre-Channel-Speicherung (optional) 18

3 Aufgaben nach der Installation 20

Verwenden einer anderen Sprache als Englisch beim Windows-Start 20
Zugriff auf die Kern-Konsole 20
Aktualisieren von vertrauenswürdigen Seiten im Internet Explorer 21
Konfigurieren von Browsern für den Remotezugriff auf die Core Console 21
Konfiguration der Browser-Einstellungen für Internet Explorer und Chrome: 22
Konfiguration von Mozilla Firefox-Browser-Einstellungen 22
Überprüfen der Beibehaltungszeiträume 23
Verschlüsseln der Agent Snapshot-Daten 23

Konfigurieren eines E-Mail-Servers und einer E-Mail-Benachrichtigungsvorlage 24
Anpassen der Anzahl der Streams..... 25
Das Schützen von Maschinen und das Überprüfen der Client-Konnektivität..... 25
Überprüfen der Netzwerk-Verbindungsfähigkeit..... 26
Überprüfen der Firewall-Einstellungen..... 26
Überprüfen der Namensauflösung (falls vorhanden)..... 27
Teaming von Netzwerkkarten..... 27
Neuinstallation der Broadcom Advanced Configuration Suite (Software-Suite für die erweiterte Broadcom-Konfiguration)..... 27
Erstellung des NIC-Teams..... 27

4 Installieren von Agenten auf Clients..... 29
Remote-Installation von Agenten (Push)..... 29
Bereitstellen der Agentensoftware beim Schutz eines Agenten..... 30
Installieren von Microsoft Windows-Agenten auf dem Client..... 31
Hinzufügen eines Agenten durch Verwenden des Lizenzportals..... 32
Installieren von Agenten auf Linux-Maschinen..... 32
Speicherort der Linux-Agenten-Dateien..... 33
Agenten-Abhängigkeiten..... 34
Installieren des Agenten auf Ubuntu..... 35
Installation des Agenten auf Red Hat Enterprise Linux und CentOS..... 35
Installieren des Agenten auf SUSE Linux Enterprise Server..... 36

5 Wie Sie Hilfe bekommen..... 37
Ausfindig machen der Dokumentation und Software-Aktualisierungen..... 37
Softwareaktualisierungen..... 37
Kontaktaufnahme mit Dell..... 37
Feedback zur Dokumentation..... 37

1

Einrichten des DL4300-Geräts

Einführung

Das Dell DL4300-Gerät ist die neueste Generation eines Backup-to-Disk-Sicherungsgeräts mit Unterstützung von Dell AppAssure-Software. Das Gerät ermöglicht Folgendes:

- Skalierbare Speicherfunktionen zur Unterstützung von Organisationen jeglicher Größe
- Schnellere Sicherungen sowie schnellere Wiederherstellungsszenarien über herkömmliche Bandgeräte und Sicherungsmethoden.
- Optionale Möglichkeit zur Deduplizierung
- Permanenter Datenschutz für Rechenzentren und Server in Betriebsniederlassungen
- Schnelle und einfache Bereitstellung, dank der wichtige Daten sofort geschützt werden können
- Optional: Fibre-Channel-Konfiguration

Verfügbare Konfigurationen

Die DL Appliance wird in zwei Konfigurationen geliefert: Standard Edition und High Capacity Edition.

Tabelle 1. Kapazitätskonfigurationen der Standard Edition für DL4300

Kapazität	Hardwarekonfiguration
5 TB	Laufwerke 12 x 1 TB, interne Laufwerke: 4 x 1 TB
10–20 TB	Laufwerke 12 x 2 TB, interne Laufwerke: 4 x 2 TB
30–40 TB	Laufwerke 12 x 4 TB, interne Laufwerke: 4 x 4 TB
50 bis 60 TB	Laufwerke 12 x 6 TB, interne Laufwerke: 4 x 6 TB

Tabelle 2. Kapazitätskonfigurationen der High Capacity Edition von DL4300

Kapazität	Hardwarekonfiguration
40 TB, 50 TB, 60 TB, 70 TB, 80 TB, 90 TB, 100 TB, 110 TB und 120 TB	Laufwerke 12 x 6 TB, interne Laufwerke: 4 x 6 TB

ANMERKUNG: Zusätzlicher Speicher kann durch Erweiterungsfächer hinzugefügt werden (Dell Storage MD1400). Zusätzlicher Speicher kann zu jedem beliebigen Modell hinzugefügt werden, die Standard Edition hat jedoch eine maximale Kapazität von 60 TB und die High Capacity Edition hat eine maximale Kapazität von 120 TB. Beide Editionen erlauben bis zu maximal vier Erweiterungsgehäuse.

Jede Konfiguration umfasst die folgende Hard- und Software:

- Dell DL4300-System
- Dell PowerEdge RAID-Controller (PERC)
- Vorinstalliertes Betriebssystem sowie Dell OpenManage-System- und Speicherverwaltungssoftware.
- AppAssure-Software

ANMERKUNG: Wenn die Gerätekonfiguration keine Dell Storage MD1400-Speichergehäuse umfasst, können Sie die in diesem Dokument genannten Referenzen zu Dell Storage MD1400 und zu den Speichergehäusen ignorieren.

In diesem Dokument verwendete Begriffe

Die folgende Tabelle führt die in diesem Dokument verwendeten Begriffe auf, um auf verschiedene Hard- und Software-Komponenten des DL4300-Geräts Bezug zu nehmen.

Tabelle 3. Hard- und Software-Komponenten des DL4300-Geräts

Komponente	Verwendete Begriffe
DL4300-Gerät	Appliance
Dell Storage MD1400-Speichergehäuse	Speichergehäuse
Dell AppAssure Software	AppAssure

Installationsvoraussetzungen

Netzwerkanforderungen

Für Ihr Gerät muss die folgende Netzwerkumgebung vorhanden sein:

- Aktives Netzwerk mit verfügbaren Ethernet-Kabeln und -Verbindungen
- Eine statische IP-Adresse und die IP-Adresse eines DNS-Servers, falls nicht durch DHCP (Dynamic Host Configuration Protocol) zugewiesen
- Benutzername und Kennwort mit Administratorrechten

Empfohlene Netzwerkinfrastruktur

Dell empfiehlt Organisationen die Verwendung von1 GbE Backbone für eine effiziente Leistung bei der Verwendung von AppAssure und 10 GbE-Netzwerke für extrem stabile Umgebungen.

Einrichten der Hardware

Das Gerät wird mit einem einzelnen DL4300-System geliefert. Lesen Sie vor dem Einrichten der Gerätehardware das Dokument *Dell DL4300 Appliance Getting Started With Your System* (Erste Schritte für das Dell DL4300-Gerät), das im Lieferumfang des Geräts enthalten ist. Packen Sie dann die DL-Gerätehardware aus, und richten Sie diese ein.

ANMERKUNG: Die Software ist auf dem System vorinstalliert. Sämtliche im System enthaltenen Datenträger dürfen nur dann verwendet werden, wenn eine Systemwiederherstellung erforderlich ist.

So richten Sie die DL Appliance-Hardware ein:

1. Montieren Sie das DL4300-System und das bzw. die Speichergehäuse, und verkabeln Sie alle Geräte.
2. Schalten Sie das bzw. die Speichergehäuse und anschließend das DL4300-System ein.

Installation des Systems in einem Rack

Wenn Ihr System ein Schienen-Kit beinhaltet, machen Sie die *Rack Installation Instructions* (Anweisungen für die Rack-Installation) ausfindig, die mit dem Schienen-Kit mitgeliefert werden. Befolgen Sie die Anweisungen, um die Schienen in der Rackeinheit, das System und das Speichergehäuse im Rack zu installieren.

Einstellen des Konfigurationsschalters für das Speichergehäuse

Stellen Sie den Speichermodus für das Speichergehäuse auf den einheitlichen Modus ein, wie in der folgenden Abbildung gezeigt.

ANMERKUNG: Der Konfigurationsschalter muss vor dem Einschalten des Speichergehäuses eingestellt werden. Wird der Konfigurationsmodus nach Einschalten des Speichergehäuses geändert, hat dies erst dann eine Auswirkung auf die Gehäusekonfiguration, wenn das System aus- und wieder eingeschaltet wurde. Weitere Informationen siehe *Dell Storage MD1400 Enclosures Hardware Owner's Manual* (Hardware-Benutzerhandbuch für Dell Storage MD1400-Gehäuse) unter **support.dell.com/home**.

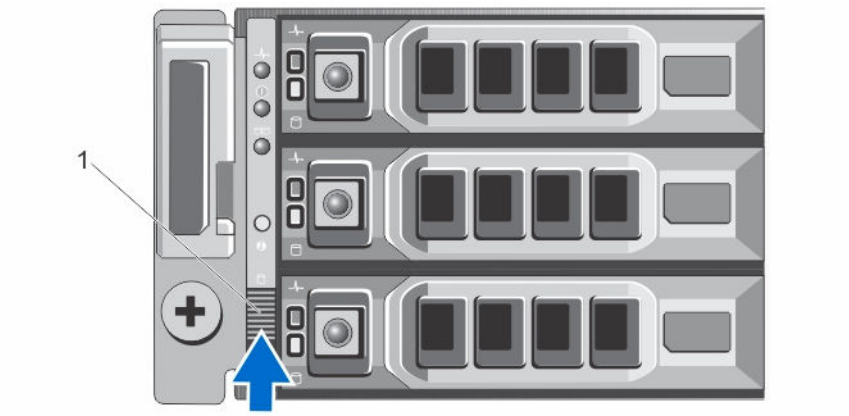


Abbildung 1. Einstellen des Konfigurationsschalters für das PowerVault MD1400-Speichergehäuse

1. Konfigurationsschalter

Anschließen des Speichergehäuses an das System

Schließen Sie das Datenkabel des auf dem DL4300-System installierten PowerEdge RAID-Controllers (PERC) an den primären Enclosure Management Module (EMM)-SAS-Anschluss am Speichergehäuse an.

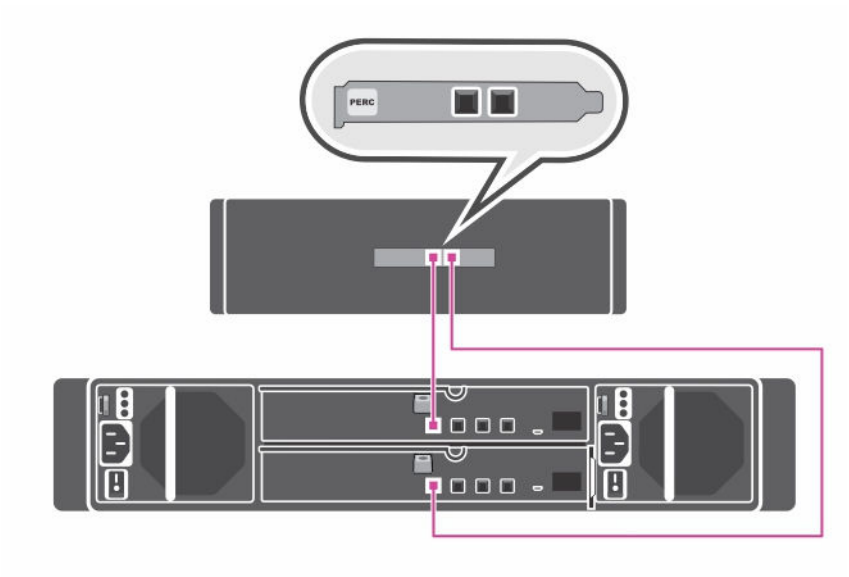


Abbildung 2. Anschließen des DL4300-Systems an das MD1400 Speichergehäuse.

Redundante Port-Konfiguration

Für redundante Port-Konfiguration:

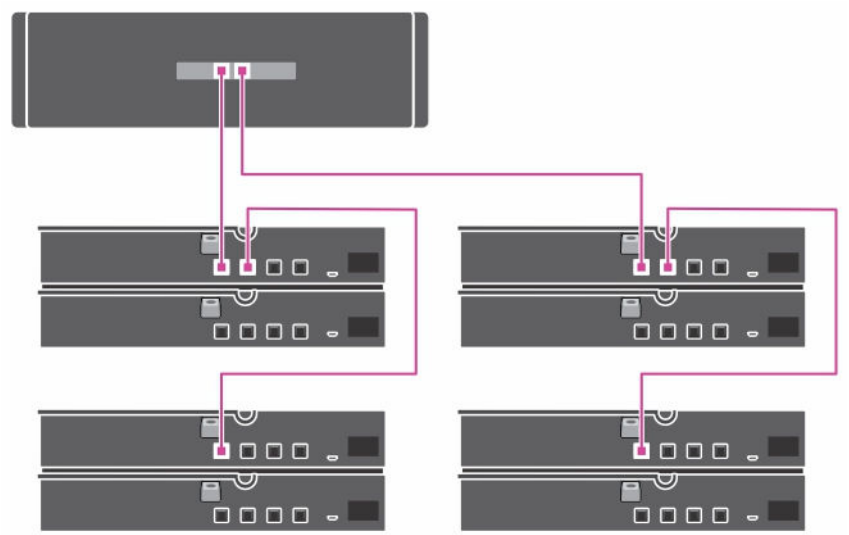
1. Verbinden Sie das eine Ende jedes SAS-Kabels mit Port 0 und Port 1 am DL4300 System-PERC-Controller.
2. Verbinden Sie das andere Ende jedes SAS-Kabels mit Port 1 eines jeden Enclosure Management Module (EMM) am MD1400-Speichergehäuse.

Single-Port-Konfiguration

Für Single-Port-Konfiguration:

1. Verbinden Sie das eine Ende des SAS-Kabels mit Port 0 am DL4300 System-PERC-Controller.
2. Verbinden Sie das andere Ende des SAS-Kabels mit Port 1 des Enclosure Management Module (EMM) am MD1400-Speichergehäuse.

Multi-Chain-Konfiguration



Die Multi-Chain-Konfiguration unterstützt bis zu vier Gehäuse. Die ersten zwei Gehäuse sind in Reihe mit einem der Gehäuse verbunden, die an einen einzelnen Port auf der Controller-Karte angeschlossen sind. Die anderen zwei Gehäuse sind in Reihe mit einem der Gehäuse verbunden, die an den zweiten Port auf der Controller-Karte angeschlossen sind.

Anschließen des Kabelführungsarms (optional)

Falls Ihr System einen Kabelführungsarm (CMA) enthält, machen Sie die *Installationsanleitung für den Kabelführungsarm* ausfindig, die im Lieferumfang des Kits mit dem Kabelführungsarm enthalten ist, und befolgen Sie die Anweisungen zum Installieren des Kabelführungsarms.

Verkabelung des Systems

Machen Sie das Dokument *Getting Started With Your System* (Erste Schritte) ausfindig, das im Lieferumfang des Geräts enthalten ist. Folgen Sie den Anweisungen zum Anschließen der Tastatur-, Maus-, Monitor-, Strom- und Netzwerkkabel an das Gerät.

Einschalten des Systems

Schalten Sie nach dem Verkabeln des Geräts das MD1400-Speichergehäuse ein, und schalten Sie anschließend das DL4300-System ein.

ANMERKUNG: Es wird empfohlen, das System für maximale Zuverlässigkeit und Verfügbarkeit an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen.

DL4300-Laufwerkskonfigurationen

DL4300 unterstützt ausschließlich Nearline-SAS-Laufwerke. Das Betriebssystem befindet sich auf einem (gespiegelten) virtuellen RAID 1-Laufwerk, das auf den Steckplätzen 12 und 13 befindet. Weitere Informationen zu diesen Laufwerken siehe *Dell DL4300 Appliance Owner's Manual* (Benutzerhandbuch für das Gerät) unter **dell.com/support/home**. Die in den Steckplätzen 0–11 und 14–17 verfügbaren Laufwerke stehen für eine automatische Konfiguration von AppAssure Appliance Configuration Wizard (AppAssure-Gerätekonfigurationsassistenten, empfohlen) bereit, können aber auch nach Bedarf für benutzerdefinierte Konfigurationen manuell konfiguriert werden. Die Laufwerke werden automatisch als RAID 6 bereitgestellt. Eine Kapazitätserweiterung unter Nutzung eines MD1400-Speichergehäuses ist optional.

2

Anfänglicher Software-Setup

Nach dem ersten Einschalten des Geräts und Ändern des Systemkennworts wird automatisch der **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistent) ausgeführt.

1. Nach dem Einschalten des Systems wird der Microsoft-Endbenutzer-Lizenzvertrag (EULA) auf der Seite **Einstellungen** angezeigt.

   VORSICHT: Achten Sie darauf, dass Sie alle Schritte des AppAssure Appliance Configuration Wizard (AppAssure-Gerätekonfigurationsassistenten) befolgen, bevor Sie einen anderen Task starten oder Einstellungen der Anwendung ändern. Nehmen Sie keine Änderungen über die Systemsteuerung vor, führen Sie keine Microsoft Windows-Aktualisierung durch, aktualisieren Sie keine AppAssure-Software und installieren Sie keine Lizenzen, bevor der Assistent nicht abgeschlossen ist.

   VORSICHT: Dell DL4300 ist aktuell so entwickelt, dass es mit Englisch als Systemstandardsprache funktioniert. Wählen Sie immer Englisch als Windows-Sprache aus, und verwenden Sie keine Sprachpakete in anderen Sprachen. Die Verwendung eines Sprachpakets in einer anderen Sprache als Englisch führt zu nicht ordnungsgemäßen Systemvorgängen. Sollten Sie beim Start von Windows ein Sprachpaket in einer anderen Sprache als Englisch ausgewählt haben, finden Sie Informationen zum Rekonfigurieren des Sprachpakets zu Englisch unter Verwenden einer anderen Sprache als Englisch beim Windows-Start.
2. Übernehmen Sie die Endbenutzer-Lizenzvereinbarung, indem Sie auf **Ich stimme zu** klicken.
   Ein Bildschirm zum Ändern des Administratorkennworts wird angezeigt.
3. Klicken Sie bei der Meldung, die Sie zum Ändern Ihres Administrator-Kennworts auffordert auf **OK**.
4. Geben Sie das neue Kennwort ein und bestätigen Sie es.
   Sie werden von einer Meldung darauf hingewiesen, dass das Kennwort geändert wurde.
5. Klicken Sie auf **OK**.
6. Scrollen Sie von dem Bildschirm **Dell readme.htm** nach unten und klicken Sie auf **Fortfahren**.
7. Melden Sie sich mit dem geänderten Administratorkennwort an.

Es wird der Willkommenbildschirm des **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistent) angezeigt.

ANMERKUNG: Es kann bis zu 30 Sekunden dauern, bis der **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistent) auf der Systemkonsole angezeigt wird.

ANMERKUNG: Schließen Sie den **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistenten) erst, wenn alle Tasks abgeschlossen sind.

AppAssure-Systemkonfigurationsassistent

VORSICHT: Achten Sie darauf, dass Sie alle Schritte des AppAssure Appliance Configuration Wizard (AppAssure-Gerätekonfigurationsassistenten) befolgen, bevor Sie einen anderen Task starten oder Einstellungen der Anwendung ändern. Nehmen Sie keine Änderungen über die Systemsteuerung vor, führen Sie keine Microsoft Windows-Aktualisierung durch, aktualisieren Sie keine AppAssure-Software und installieren Sie keine Lizenzen, bevor der Assistent nicht abgeschlossen ist.

Der **AppAssure-Systemkonfigurationsassistent** führt Sie durch die weiteren Schritte zum Konfigurieren der Software im System.

- Konfiguration der Netzwerkschnittstelle
- Konfiguration der Host-Namen- und Domain-Einstellungen
- Konfigurieren der SNMP-Einstellungen
- Appliance-Schnellselbstwiederherstellung

Nach Abschluss der Installation mithilfe des Assistenten startet die Kern-Konsole automatisch.

Konfiguration der Netzwerkschnittstelle

So konfigurieren Sie die vorhandenen Netzwerkschnittstellen:

1. Klicken Sie auf dem **Begrüßungsbildschirm des AppAssure-Systemkonfigurationsassistenten** auf **Weiter**.

   Die Seite **Netzwerkschnittstellen** zeigt die verfügbaren verbundenen Netzwerkschnittstellen an.
2. Wählen Sie die Netzwerkschnittstellen aus, die Sie konfigurieren wollen.

   ANMERKUNG: Der **AppAssure-Systemkonfigurationsassistent** konfiguriert Netzwerkschnittstellen als einzelne Ports (ohne Teaming). Für eine Verbesserung der Aufnahmeleistung können Sie einen größeren Aufnahmekanal durch Teaming der NICs erstellen. Dies muss jedoch nach der Erstkonfiguration des Systems vorgenommen werden.
3. Falls erforderlich, verbinden Sie die zusätzlichen Nezwerkschnittstellen und klicken Sie auf **Aktualisieren**.

   Die zusätzlich verbundenen Netzwerkschnittstellen werden angezeigt.
4. Klicken Sie auf **Weiter**.

   Es wird die Seite **Ausgewählte Netzwerkschnittstelle konfigurieren** angezeigt.
5. Wählen Sie für die ausgewählte Schnittstelle das entsprechende Internetprotokoll aus.

   Sie können **IPv4** oder **IPv6** auswählen.

   Es werden die Netzwerkeinzelheiten entsprechend Ihrer Auswahl des Internetprotokolls angezeigt.
6. Verwenden Sie zum Zuweisen der Internetprotokolleinzelheiten eine der folgenden Vorgehensweisen:
   - Wählen Sie zum automatischen Zuweisen der Internetprotokolleinzelheiten **IPV4-Adresse automatisch beziehen**.
   - Wählen Sie zum manuellen Zuweisen der Netzwerkverbindung **Folgende IPv4-Adresse verwenden** aus und geben Sie die folgenden Details ein:
     - **IPv4 Adresse** oder **IPv6-Adresse**

- **Subnetzmaske** für IPv4 und **Subnetzpräfixlänge** für IPv6
- **Standard-Gateway**

7. Verwenden Sie zum Zuweisen der DNS-Server-Einzelheiten eine der folgenden Vorgehensweisen:
   - Wählen Sie zum automatischen Zuweisen der DNS-Server-Einzelheiten **DNS-Server-Adresse automatisch beziehen**.
   - Wählen Sie zum manuellen Zuweisen des DNS-Servers **Folgende DNS-Server-Adresse verwenden** und geben Sie die folgenden Details ein:
     - **Bevorzugter DNS-Server**
     - **Alternativer DNS-Server**
8. Klicken Sie auf **Weiter**.

   Es wird die Seite **Hostnamen- und Domain-Einstellung** angezeigt.

Weitere Informationen zu NIC-Teamvorgang finden Sie unter Teaming von Netzwerkkarten.

Konfiguration der Host-Namen- und Domain-Einstellungen

Dem System muss ein Host-Name zugewiesen werden. Es wird empfohlen, dass der Host-Name geändert wird, bevor Sicherungen gestartet werden. Standardmäßig ist der Host-Name der Systemname, wie er durch das Betriebssystem zugewiesen wird.

ANMERKUNG: Wenn Sie vorhaben, den Host-Namen zu ändern, wird empfohlen, dass Sie den Host-Namen zu diesem Zeitpunkt ändern. Das Ändern des Host-Namens nach Abschluss des **AppAssure-Systemkonfigurationsassistent** erfordert die manuelle Durchführung mehrerer Schritte.

Konfigurieren Sie den Host-Namen und die Domäneneinstellungen:

1. Ändern Sie den Host-Namen des Systems auf der Seite **Host-Namen- und Domain-Einstellungen konfigurieren.** Geben Sie zum Ändern des Host-Namens des Systems in **Neuer Host-Name** einen geeigneten Host-Namen ein.
2. Wenn Sie nicht wollen, dass das System einer Domain beitritt, dann wählen Sie in **Wollen Sie, dass dieses System einer Domain beitritt? Nein** aus

   Standardmäßig ist **Ja** voreingestellt.
3. Geben Sie die folgenden Einzelheiten ein, um das System einer Domain beitreten zu lassen:
   - **Domänenname**
   - **Domain-Benutzername**

     ANMERKUNG: Der Domain-Benutzername muss über lokale Administratorrechte verfügen.
   - **Domain-Benutzerkennwort**
4. Klicken Sie auf **Weiter**.

   ANMERKUNG: Das Ändern des Host-Namens oder der Domain erfordert einen Neustart der Maschine. Nach dem Neustart der Maschine wird automatisch der **AppAssure-Systemkonfigurationsassistent** gestartet. Wenn das System einer Domain beigetreten ist, müssen Sie sich nach dem Neustart als Domainnutzer mit Administratorberechtigungen am System anmelden.

   Es wird die Seite **SNMP-Einstellungen konfigurieren** angezeigt.

Konfigurieren der SNMP-Einstellungen

Simple Network Management Protocol (SNMP) ist ein häufig verwendetes Netzwerkverwaltungsprotokoll, das SNMP-kompatible Verwaltungsfunktionen ermöglicht, wie z.B. die Geräteermittlung, Überwachung und Ereignisgenerierung. SNMP bietet die Netzwerkverwaltung des TCP/IP-Protokolls.

So konfigurieren Sie SNMP-Warnungen für das Gerät:

1. Wählen Sie auf der Seite **SNMP-Einstellungen konfigurieren Auf diesem Gerät SNMP konfigurieren** [auf der Seite **SNMP-Einstellungen konfigurieren]** aus.

   ANMERKUNG: Heben Sie die Auswahl von **Auf diesem Gerät SNMP konfigurieren** auf, wenn Sie auf dem Gerät keine SNMP-Details und Warnungen einrichten wollen und fahren Sie mit Schritt 6 fort.
2. Geben Sie in **Communities** einen oder mehrere SNMP-Community-Namen ein.

   Verwenden Sie Kommas zum Trennen mehrerer Community-Namen.
3. Geben Sie in **SNMP-Pakete von diesen Hosts akzeptieren** die Namen von Hosts ein, mit denen das Gerät kommunizieren kann.

   Trennen Sie die Host-Namen mit Kommas oder lassen Sie dieses Feld unausgefüllt, um eine Kommunikation mit allen Hosts zu erlauben.
4. Geben Sie zum Konfigurieren von SNMP-Warnungen den **Community-Namen** und die **Trap-Ziele** für die SNMP -Warnungen ein und klicken Sie auf **Hinzufügen**.

   Wiederholen Sie diesen Schritt, um weitere SNMP-Adressen hinzuzufügen.
5. Wählen Sie zum Entfernen einer konfigurierten SNMP-Adresse in **Konfigurierte SNMP-Adressen** die entsprechende SNMP-Adresse aus und klicken Sie auf **Entfernen**.
6. Klicken Sie auf **Weiter**.

   Die Seite **Erstellen von Windows- und RASR-virtuellen Festplatten** wird angezeigt.

Appliance-Schnellselbstwiederherstellung

Bei der Appliance-Schnellselbstwiederherstellung (Rapid Appliance Self Recovery, RASR) handelt es sich um einen Bare-Metal-Wiederherstellungsprozess, bei dem die Laufwerke des Betriebssystems auf das werkseitig voreingestellte Image neu erstellt werden.

Erstellen von Windows- und RASR-virtuellen Festplatten

Das System DL4300 unterstützt Folgendes:

- Zwei Betriebssystemlaufwerke, zwölf Datenlaufwerke und vier interne Festplatten.
- Eine Option zum Erstellen von Logical Unit Numbers (LUNs) für die Bare-Metal-Wiederherstellung (BMR) mit den zu speichernden Informationen.
- Eine Option zum Erstellen von separaten-Speicherplatz für die Windows-Sicherung-RASR-Datei.

Zum Erstellen von virtuellen Festplatten:

1. Wählen Sie die folgenden virtuellen Festplatten aus:
   a. Windows-Sicherung der virtuellen Festplatte

Die virtuelle Festplatte des Windows-Backups stellt den Zielspeicherort für die Erstellung eines Windows Server-Backups bereit. Um einen Windows Server-Backup durchzuführen, wählen Sie auf der Seite **Backup** die Registerkarte **Appliance** (Gerät) unter AppAssure Core aus. Wenn Sie diese Option in dem **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistenten) übersprungen haben, können Sie an dieser Stelle kein Windows Server-Backup erstellen und müssen eine Backup-Richtlinie von der Seite **Backup** konfigurieren. Weitere Informationen siehe Executing the RASR through RASR USB key (Ausführen von RASR über den RASR-USB-Schlüssel).

b. Startfähiges RASR-virtuelles Laufwerk

Ein bootbares virtuelles RASR-Laufwerk stellt ein redundantes Wiederherstellungsvolume bereit, um eine RASR-Wiederherstellung durchzuführen. Sie können das redundante Wiederherstellungsvolume neu starten, indem Sie die Taste <F8> während des POST-Vorgangs drücken. Befolgen Sie nach dem Neustart die Schritte unter Executing the RASR through RASR USB key (Ausführen von RASR über den RASR-USB-Schlüssel).

2. Klicken Sie auf **Next** (Weiter).

   Ein vielen Dank-Fenster angezeigt, während das System konfiguriert wird. Eine Konfiguration ist abgeschlossen-Meldung wird angezeigt.

3. Klicken Sie auf **Exit** (Beenden).

   Die Core Console startet automatisch.

4. Fahren Sie über Provisioning Storage (Speicherbereitstellung) mit dem Konfigurationsprozess fort.

Erstellen des RASR-USB-Sticks

ANMERKUNG: Nach der Erstinstallation der Software wird der **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistent) automatisch gestartet. Das Statussymbol auf der Registerkarte **Appliance** (Gerät) wird gelb angezeigt.

So erstellen Sie einen RASR-USB-Speicherstick:

1. Navigieren Sie zur Registerkarte **Appliance** (Gerät).
2. Wählen Sie im Navigationsbereich auf der linken Seite die Optionen **Appliance (Gerät)** → **Backup** aus.

   Daraufhin wird das Fenster **Create RASR USB Drive** (RASR-USB-Laufwerk erstellen) angezeigt.

   ANMERKUNG: Fügen Sie einen 16 GB oder grösseren USB-Stick ein, bevor Sie versuchen, einen RASR-Stick zu erstellen.

3. Klicken Sie nach dem Einsetzen eines USB-Sticks mit mindestens auf **Create RASR USB Drive now** (RASR-USB-Laufwerk jetzt erstellen).

   Daraufhin wird die Meldung **Prerequisite Check** (Überprüfung der Voraussetzung) angezeigt.

   Nachdem Sie die Voraussetzungen überprüft wurden, zeigt das Fenster **Create the RASR USB Drive** (RASR-USB-Stick erstellen) die Mindestgröße für die Erstellung des USB-Laufwerks und **listet alle möglichen Zielpfade** auf.

4. Wählen Sie das Ziel aus, und klicken Sie auf **Create** (Erstellen).

   Es wird ein Warndialogfeld angezeigt.

5. Klicken Sie auf **Yes** (Ja).

   Der RASR-USB-Laufwerks-Stick wurde erstellt. Entfernen Sie den Stick, kennzeichnen Sie ihn, und heben Sie ihn für die künftige Verwendung auf.

Ausführen von RASR über den RASR-USB-Schlüssel.

So führen Sie RASR mit dem USB-Schlüssel aus:

1. Legen Sie den erstellten RASR-USB-Schlüssel ein. Weitere Informationen finden Sie unter Erstellen des RASR-USB-Schlüssels.
2. Starten Sie die Appliance über den RASR-USB-Schlüssel neu.

   Die folgende Meldung wird angezeigt:

   ```
   Die zweite SD-Karte ist nicht vorhanden, reagiert nicht oder befindet sich im schreibgeschützten Modus. Führen Sie einen der folgenden Schritte aus: 1) Installieren Sie einen SD-Kartendatenträger in den sekundären SD-Kartenleser. 2) Setzen Sie die SD-Karte neu ein oder ersetzen Sie diese. 3) Wenn Sie vermuten, dass der schreibgeschützte Modus aktiv ist, ist keine Handlungsmaßnahme erforderlich.
   ```

   Ignorieren Sie obenstehende Warnmeldung.
3. Klicken Sie auf **Troubleshoot (Fehlerbehebung)** → **Rapid Appliance Self Recovery (Appliance-Schnellselbstwiederherstellung)**.

   Das **Recovery Tool** (Wiederherstellungstool) wird angezeigt.
4. Wählen Sie die Windows-Version des Betriebssystems.

   Das Windows cmd-Fenster wird nachdem RASR-Startbildschirm angezeigt.
5. Klicken Sie auf **Next** (Weiter).

   Der Bildschirm **Prerequisites** (Voraussetzungen) wird angezeigt.

   ANMERKUNG: Stellen Sie sicher, dass alle Hardware- und sonstigen Voraussetzungen überprüft werden, bevor Sie die RASR ausführen.
6. Klicken Sie auf **Next** (Weiter).

   Der Bildschirm **Recovery Mode Selection** (Auswahl des Wiederherstellungsverfahrens) wird mit den folgenden drei Optionen angezeigt:

   - **System Recovery** (Systemwiederherstellung) – Diese Option ist per Standardeinstellung deaktiviert. Um diese Option zu aktivieren, wählen Sie **Windows Backup virtual disk** (Windows-Backup der virtuellen Festplatte) beim Erstellen der virtuellen Laufwerke unter Verwendung des **AppAssure Appliance Recovery Wizard** (Recovery-Assistent des AppAssure-Geräts) aus. Über System Recovery können Sie Windows-Backups, die auf der virtuellen Festplatte des Windows-Backups erstellt wurden, auswählen und sie für Wiederherstellungen verwenden.
   - **Windows-Recovery-Assistent** – Diese Option ist die Standardeinstellung für den Microsoft Windows-Recovery-Assistenten, der die Netzwerkfreigabe verwendet, um das Betriebssystem zu sichern.
   - **Auf Werkseinstellungen zurücksetzen** - Mit dieser Option setzen Sie den Betriebssystemdatenträger wieder auf die Werkseinstellungen zurück.
7. Wählen Sie **Factory Reset** (Auf Werkseinstellungen zurücksetzen) aus.
8. Klicken Sie auf **Next** (Weiter).

   Daraufhin wird der Bildschirm **Storage Configuration** (Speicherkonfiguration) angezeigt.
9. Im Bildschirm **OS Recovery** (Betriebssystem-Wiederherstellung) wird der RASR abgeschlossen-Bildschirm mit der folgenden Meldung angezeigt: `The system has been recovered successfully` (Das System wurde erfolgreich wiederhergestellt).
10. Klicken Sie auf **Finish** (Fertigstellen), um RASR zu beenden.

Ausführen von RASR über das interne Dual SD-Modul

Das System wird mit einem internen Dual SD-Modul und einer SD-Karte mit einer Kapazität von 16 GB geliefert.

So führen Sie RASR über das interne Dual SD-Modul (IDSDM) aus:

1. Starten Sie das Gerät über das ISDNM neu.

   VORSICHT: Achten Sie darauf, dass die SD-Karte in Steckplatz 1 eingesetzt wurde.

   Die folgende Meldung wird angezeigt.

   ```
   Die zweite SD-Karte ist nicht vorhanden, reagiert nicht oder befindet sich
   im schreibgeschützten Modus. Führen Sie einen der folgenden Schritte aus:
   1) Installieren Sie einen SD-Kartendatenträger in den sekundären SD-
   Kartenleser. 2) Setzen Sie die SD-Karte neu ein oder ersetzen Sie diese. 3)
   Wenn Sie vermuten, dass der schreibgeschützte Modus aktiv ist, ist keine
   Handlungsmaßnahme erforderlich.
   ```

   Ignorieren Sie obenstehende Warnmeldung.
2. Um RASR weiterhin über das interne SD-Modul auszuführen, führen Sie Schritt 3 bis Schritt 10 des Abschnitts Executing the RASR through RASR USB key (Ausführen von RASR über den RASR-USB-Schlüssel) aus.

Speicherbereitstellung

Das Gerät konfiguriert automatisch den im DL4300 intern verfügbaren Speicher und alle verbundenen externen Speichergehäuse für:

- AppAssure-Repositories

  ANMERKUNG: Wenn Fibre Channel-HBA konfiguriert ist, ist das Erstellen der Repositorys ein manueller Prozess. AppAssure erstellt kein Repository automatisch im Stammverzeichnis. Weitere Informationen siehe *Dell DL4300Appliance Deployment Guide* (Bereitstellungshandbuch für das Dell DL4300-Gerät).
- Virtuelles Standby der geschützten Maschinen

ANMERKUNG: MD1400s mit 1TB-, 2TB-, 4TB-, oder 6TB-Laufwerken (für hohe Kapazitäten), die mit dem H830-Controller verbunden sind, werden unterstützt. Bis zu vier MD1400s werden unterstützt.

ANMERKUNG: Die DL4300-Konfiguration mit hoher Kapazität unterstützt entweder H830 -PERC-SAS-Adapter oder zwei Fibre Channel-HBAs. Weitere Informationen zur Konfiguration von Fibre Channel-HBAs finden Sie im entsprechenden Whitepaper zur FC-Implementierung *DL4xxx – Fibre Channel Implementation* unter **dell.com/support/home**.

Bevor Sie Speicher auf dem Laufwerk bereitstellen, müssen Sie bestimmen, wie viel Speicher Sie für die virtuellen Standby-Maschinen brauchen. Sie können einen beliebigen Prozentsatz der verfügbaren Kapazität für das Hosten virtueller Standby-Maschinen zuordnen. Wenn Sie zum Beispiel Storage Resource Management (SRM) verwenden, können Sie bis zu 100 Prozent Kapazität auf ein Gerät, das auf virtuelle Maschinen bereitgestellt ist, zuordnen. Diese Maschinen können unter Verwendung der Live Recovery-Funktion von AppAssure verwendet werden, um beliebige Server wiederherzustellen, die durch das Gerät geschützt werden.

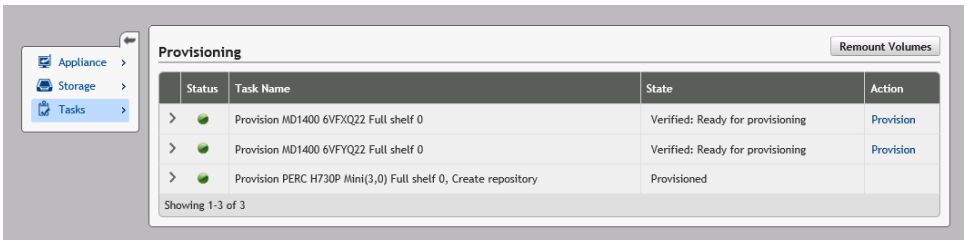
Basierend auf einer mittelgroßen Umgebung die keine virtuellen Standby-Maschinen braucht, können Sie den ganzen Speicher dazu verwenden eine erhebliche Anzahl von Agenten zu sichern. Wenn Sie jedoch weitere Ressourcen für virtuelle Standby-Maschinen benötigen und eine kleinere Anzahl von Agentenmaschinen sichern, können Sie den größeren VMs mehr Ressourcen zuweisen.

Wenn Sie die Registerkarte **Appliance** (Geräte) auswählen, findet die AppAssure Appliance-Software den verfügbaren Speicher für alle unterstützten Controller im System und bestätigt, dass die Hardware den Anforderungen entspricht.

So schließen Sie die Laufwerksbereitstellung für alle verfügbaren Speicher ab:

1. Klicken Sie in der Registerkarte **Appliance** (Gerät) auf **Tasks** → **Provisioning (Bereitstellung)**.
   Der Bildschirm **Provisioning** (Bereitstellung) zeigt die erwartete Kapazität der Speicherzuweisung an. Diese Kapazität wird dazu verwendet, ein neues AppAssure-Repository zu erstellen.

   VORSICHT: Bevor Sie fortfahren, stellen Sie sicher, dass Sie Schritt 2 bis 4 dieses Verfahrens ausgeführt haben.
2. Öffnen Sie das Fenster **Speicherbereitstellung**, indem Sie in der Aktionsspalte neben dem Speicher, den Sie bereitstellen möchten, auf **Bereitstellung** klicken.
3. Markieren Sie im Abschnitt **Optionale Speicherreserve** das Kontrollkästchen **Einen Teil des Speichers zuweisen, der für virtuelle Standby-Maschinen und andere Zwecke bereitgestellt wird**, und geben Sie einen Prozentsatz des zuzuweisenden Speichers an. Andernfalls wird der Prozentsatz des Speichers, der im Abschnitt **Optionale Speicherreserve** angegeben ist, von allen angeschlossenen Festplatten entnommen.
4. Klicken Sie auf **Provision** (Bereitstellung)



Konfiguration von DL4300 unter Verwendung der Fibre-Channel-Speicherung (optional)

Die Edition mit hoher Kapazität von DL4300 bietet eine Fibre-Channel-HBA-Storage-Option, die das Erstellen von Repositorys unter Verwendung von Fibre-Channel-Speicher-Arrays ermöglicht.

ANMERKUNG: Wenn die Fibre-Channel-Konfiguration bestellt wird, ersetzt sie den steckplatzgebundenen H830-PERC-SAS-Adapter.

ANMERKUNG: Voraussetzungen, Annahmen und detaillierte Informationen zu den folgenden Schritten finden Sie im Whitepaper *DL4xxx – Fibre Channel Implementation* (DL4xxx – Implementierung von Fibre-Channel) **dell.com/support/home** .

So integrieren und konfigurieren Sie DL4300 unter Verwendung des Fibre-Channel-Speichers:

1. Verbinden Sie DL4300-Fibre-Channel-HBA mit einem SAN-Switch.
2. Installieren Sie entweder die QLogic- oder Emulex-HBAs-Management-Software für einen Adapter, der mit dem System bestellt wurde.

3. Installieren Sie die Speicher-Array-Multipath-Software.
4. Führen Sie das Fibre-Channel-Zoning durch.
5. Erstellen Sie eine Fibre-Channel-LUN, die einem DL4300-Repository zugewiesen und als eines verwendet wird.
6. Laden Sie die Fibre Channel-LUN.
7. Konfigurieren Sie den DL4300-Fibre-Channel-Speicher als Backup-Repository.

3

Aufgaben nach der Installation

Führen Sie nach Abschluss des **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistenten) die folgenden Verfahren durch, um sicherzustellen, dass Ihr Back-up-Gerät und die durch das Gerät gesicherten Server korrekt konfiguriert wurden.

ANMERKUNG: Das Gerät ist mit einer vorläufigen, für 30 Tage gültigen Softwarelizenz für AppAssure konfiguriert. Um einen permanenten Lizenzschlüssel anzufordern, melden sie Sich im AppAssure-Lizenzportal von Dell unter **www.dell.com/DLActivation** an. Weitere Informationen zum Ändern des Lizenzschlüssels in der AppAssure-Software siehe Abschnitt „Changing A License Key" (Ändern eines Lizenzschlüssels) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät) unter **dell.com/support/home**.

Verwenden einer anderen Sprache als Englisch beim Windows-Start

Wenn Sie beim Start von Windows eine andere Sprache als Englisch ausgewählt haben, funktioniert das System nicht einwandfrei.

Zum Rekonfigurieren der Standardsprache des Systems in Englisch:

1. Melden Sie sich als Administrator an und öffnen Sie ein Befehlsfenster.
2. Navigieren Sie zu **c:\windows\system32\sysprep** und führen Sie den Befehl **sysprep.exe/generalize/oobe/reboot** aus.
3. Wählen Sie folgendermaßen:
   - **Englisch** als Sprache
   - **Vereinigte Staaten** als Land/Region
   - **US** als Tastaturlayout

   ANMERKUNG: Es wird dringend empfohlen, dass Sie den Hostnamen durch Verwendung des **AppAssure-Systemkonfigurationsassistenten** ändern. Sobald der **AppAssure-Systemkonfigurationsassistent** beendet wurde, ändern Sie den Computernamen manuell auf den vorherigen Namen zurück.

Zugriff auf die Kern-Konsole

Stellen Sie sicher, dass Sie vertrauenswürdige Seiten gemäß Abschnitt Aktualisieren von vertrauenswürdigen Seiten in Internet Explorer aktualisieren und den Browser gemäß Abschnitt Konfigurieren des Browsers für Remote-Zugriff auf die Kern-Konsole konfigurieren. Nachdem Sie die vertrauenswürdigen Seiten in Internet Explorer aktualisiert und Ihren Browser konfiguriert haben, führen Sie einen der folgenden Schritte aus, um auf die Kern-Konsole zuzugreifen:

- Melden Sie sich lokal bei Ihrem AppAssure-Kernserver an und klicken Sie dann doppelt auf das Symbol **Kern-Konsole**.
- Geben Sie eine der folgenden URLs in den Webbrowser ein:
  - **https://<yourCoreServerName>:8006/apprecovery/admin/core oder**
  - **https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core**

Aktualisieren von vertrauenswürdigen Seiten im Internet Explorer

So aktualisieren Sie vertrauenswürdige Seiten im Internet Explorer:

1. Öffnen Sie Internet Explorer.
2. Wenn die **File** (Datei) **Edit View** (Anzeige bearbeiten) und andere Menüs nicht angezeigt werden, drücken Sie auf <F10>.
3. Klicken Sie auf das Menü **Tools** (Extras) und wählen Sie **Internet Options** (Internetoptionen) aus.
4. Klicken Sie im Fenster **Internet Options** (Internetoptionen) auf die Registerkarte **Security** (Datenschutz).
5. Klicken Sie auf **Trusted Sites** (Vertrauenswürdige Seiten) und klicken Sie dann auf **Sites** (Seiten).
6. Geben Sie in **Add this website to the zone** (Diese Website zur Zone hinzufügen) unter Verwendung des Namens, den Sie als Anzeigenamen bereitgestellt haben, Folgendes ein: **https://[Display Name]** (https://[Anzeigenamen]).
7. Klicken Sie auf **Add** (Hinzufügen).
8. Geben Sie in **Add this website to the zone**, (Diese Website zur Zone hinzufügen) Folgendes ein: **about:blank**.
9. Klicken Sie auf **Add** (Hinzufügen).
10. Klicken Sie auf **Close** (Schließen) und dann auf **OK**.

Konfigurieren von Browsern für den Remotezugriff auf die Core Console

Für den Zugriff auf die Core Console von einer Remote-Maschine müssen Sie Ihre Browser-Einstellungen anpassen.

ANMERKUNG: Melden Sie sich zum Ändern der Browser-Einstellungen als Administrator am System an.

ANMERKUNG: Google Chrome verwendet Microsoft Internet Explorer-Einstellungen, ändern Sie die Einstellungen für den Chrome-Browser über den Internet Explorer.

ANMERKUNG: Stellen Sie sicher, dass die Option **Internet Explorer Enhanced Security Configuration** (Verstärkte Sicherheitskonfiguration für Internet Explorer) eingeschaltet ist, wenn Sie entweder lokal oder remote auf die Core-Web-Konsole zugreifen. So schalten Sie die Option **Internet Explorer Enhanced Security Configuration** (Verstärkte Sicherheitskonfiguration für Internet Explorer) ein:

1. Öffnen Sie den **Server-Manager**.
2. Wählen Sie die Option **Local Server IE Enhanced Security Configuration** (Verstärkte Sicherheitskonfiguration für Internet Explorer für lokale Server) auf der rechten Seite aus. Stellen Sie sicher, dass sich die Option in der Position **On** (Ein) befindet.

Konfiguration der Browser-Einstellungen für Internet Explorer und Chrome:

So ändern Sie Browser-Einstellungen für Internet Explorer und Chrome:

1. Öffnen Sie Internet Explorer.
2. Wählen Sie im Menü **Tools** (Extras) die Option **Internet Options** (Internetoptionen) auf der Registerkarte **Security** (Sicherheit) aus.
3. Klicken Sie auf **Trusted Sites** (Vertrauenswürdige Seiten) und klicken Sie dann auf **Sites** (Seiten).
4. Deaktivieren Sie die Option **Require server verification (https:) for all sites in the zone** (Serverüberprüfung erforderlich (https:) für alle Websites in der Zone), und fügen Sie dann http://*<Host-Name oder IP-Adresse des Geräteservers, der den AppAssure-Kern hostet>* zu **Trusted Sites** (Vertrauenswürdige Sites) hinzu.
5. Klicken sie auf **Close** (Schließen), wählen Sie **Trusted Sites** (Vertrauenswürdige Sites) aus und klicken Sie dann auf **Custom Level** (Benutzerdefinierte Stufe).
6. Scrollen Sie zu **Miscellaneous** → **Display Mixed Content** (Verschiedenes → Gemischten Inhalt anzeigen) und klicken Sie auf **Enable** (Aktivieren).
7. Scrollen Sie auf dem Bildschirm nach unten zu **User Authentication** → **Logon** (Benutzerauthentifizierung → Anmelden) und wählen Sie dann **Automatic logon with current user name and password** (Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort).
8. Klicken Sie auf **OK** und wählen Sie dann die Registerkarte **Advanced** (Erweitert).
9. Scrollen Sie zu **Multimedia** und wählen Sie **Play animations in webpages** (Auf Webseiten Animationen abspielen) aus.
10. Scrollen Sie zu **Security** (Sicherheit), markieren Sie **Enable Integrated Windows Authentication** (Integrierte Windows-Authentifizierung) und klicken Sie dann auf **OK**.

Konfiguration von Mozilla Firefox-Browser-Einstellungen

ANMERKUNG: Um die Mozilla Firefox-Browser-Einstellungen in den neuesten Versionen von Firefox zu ändern, muss der Schutz deaktiviert werden. Klicken Sie mit der rechten Maustaste auf die Schaltfläche „Site Identify" (Site identifizieren) (auf der linken Seite der URL), klicken Sie auf **Options** (Optionen) und dann auf **Disable protection for now** (Schutz vorübergehend deaktivieren).

So ändern Sie die Mozilla Firefox-Browser-Einstellungen:

1. Geben Sie in die Firefox-Adresszeile **about:config** ein und klicken Sie dann, wenn aufgefordert, auf **I'll be careful, I promise** (Ich verspreche, ich werde vorsichtig sein).
2. Suchen Sie nach dem Begriff **ntlm**.

   Die Suche sollte mindestens drei Ergebnisse aufzeigen.
3. Doppelklicken Sie auf **network.automatic-ntlm-auth.trusted-uris** und geben Sie die folgende Einstellung entsprechend Ihrer Maschine ein:

- Geben Sie für lokale Maschinen den Hostnamen ein.
- Geben Sie für Remote-Maschinen den Hostnamen oder die IP-Adresse des Gerätessystems, das den AppAssure-Kern hostet, durch ein Komma getrennt ein, zum Beispiel *IP-Adresse*, *Hostname*.

4. Starten Sie Firefox neu.

Überprüfen der Beibehaltungszeiträume

AppAssure legt Standard-Beibehaltungszeiträume fest, die bestimmen, wie oft Snapshots erstellt werden und wie lange die Snapshots beibehalten werden. Die Beibehaltungszeiträume müssen jedoch auf den Anforderungen Ihrer Umgebung basieren. Wenn Sie z.B. Server sichern, die unternehmenskritische Daten ausführen, die häufigen Änderungen unterliegen und für die Geschäftskontinuität unerlässlich sind, dann müssen Snapshots häufiger erstellt werden.

Zum Überprüfen und Ändern der Beibehaltungszeiträume:

1. Öffnen Sie die Core Console.
2. Wählen Sie die Registerkarte **Konfiguration** aus, und klicken Sie dann auf **Beibehaltungsrichtlinie**.
3. Passen Sie die Beibehaltungsrichtlinie basierend auf den Anforderungen Ihrer Organisation an.
4. Klicken Sie auf **Anwenden**.

Verschlüsseln der Agent Snapshot-Daten

Der Kern kann Agenten-Snapshot-Daten im Repository verschlüsseln. Anstelle einer Verschlüsselung des gesamten Repositorys wird Ihnen die Spezifizierung eines Verschlüsselungsschlüssels während des Schutzes eines Agenten in einem Repository ermöglicht, was eine erneute Verwendung des Schlüssels für verschiedene Agenten erlaubt.

Zum Verschlüsseln von Agenten-Snapshot-Daten:

1. Klicken Sie vom AppAssure-Kern auf **Konfiguration** → **Verwalten** → **Sicherheit**.
2. Klicken Sie auf **Maßnahmen**, und klicken Sie dann auf **Verschlüsselungsschlüssel hinzufügen**.
   Es wird die Seite **Verschlüsselungsschlüssel erstellen** angezeigt.
3. Vervollständigen Sie die folgenden Informationen:

Feld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein.
Kommentar	Geben Sie eine Anmerkung für den Verschlüsselungsschlüssel ein. Sie wird zur Bereitstellung zusätzlicher Details für den Verschlüsselungsschlüssel genutzt.
Passphrase	Geben Sie eine Passphrase ein. Sie wird zur Steuerung des Zugriffs verwendet.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

ANMERKUNG: Es wird empfohlen, dass Sie die Verschlüsselungspassphrase speichern, da der Verlust der Passphrase die Daten unzugänglich macht.

Konfigurieren eines E-Mail-Servers und einer E-Mail-Benachrichtigungsvorlage

Sollten Sie E-Mail-Benachrichtigungen über Ereignisse erhalten wollen, konfigurieren Sie einen E-Mail-Server und eine E-Mail-Benachrichtigungsvorlage.

ANMERKUNG: Sie müssen ebenfalls die Benachrichtigungsgruppen-Einstellungen einschließlich der Option **Notify by email** (Per E-Mail benachrichtigen) konfigurieren, bevor E-Mail-Benachrichtigungen gesendet werden. Weitere Informationen zum Festlegen von Ereignissen zum Empfangen von E-Mail-Warnungen siehe „Configuring Notification Groups For System Events" (Konfigurieren von Benachrichtigungsgruppen für Systemereignisse) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät).

So konfigurieren Sie einen E-Mail-Server und eine E-Mail-Benachrichtigungsvorlage:

1. Wählen Sie im Kern die Registerkarte **Configuration** (Konfiguration) aus.
2. Klicken Sie unter **Manage** (Verwalten) auf die Option **Events** (Ereignisse).
3. Klicken Sie im Fensterbereich **Email SMTP Settings** (E-Mail-SMTP-Einstellungen) auf **Change** (Ändern).

   Das Dialogfeld **Email Notification Configuration** (Konfiguration der E-Mail-Benachrichtigung) wird angezeigt.
4. Wählen Sie **Enable Email Notifications** (E-Mail-Benachrichtigungen aktivieren) aus und geben dann die E-Mail-Serverdetails, wie folgend beschrieben, ein:

Textfeld	Beschreibung
SMTP-Server	Geben Sie den Namen des E-Mail-Servers, der von der E-Mail-Benachrichtigungsvorlage verwendet werden soll, ein. Die Benennungskonvention umfasst Hostname, Domain und Suffix; z.B. **smtp.gmail.com.**
Schnittstelle	Geben Sie eine Schnittstellennummer ein. Sie wird zur Identifizierung der Schnittstelle für den E-Mail-Server verwendet. Zum Beispiel ist die Schnittstelle 587 für Gmail. Die Standardeinstellung ist 25.
Zeitüberschreitung (Sekunden)	Geben Sie einen Wert ein, um festzulegen, wie lange ein Verbindungsaufbau versucht wird, bevor eine Zeitüberschreitung eintritt. Diese Option wird zur Festlegung der Zeit in Sekunden verwendet, bevor beim Versuch, eine Verbindung mit dem E-Mail-Server herzustellen, eine Zeitüberschreitung eintritt. Die Standardeinstellung ist 30 Sekunden.
TLS	Verwenden Sie diese Option, wenn der E-Mail-Server eine sichere Verbindung, wie Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) verwendet.
Benutzername	Geben Sie einen Benutzernamen für den E-Mail-Server ein.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den E-Mail-Server ein.

Textfeld	Beschreibung
Von	Geben Sie eine Absender-E-Mail-Adresse ein. Diese Option wird zur Angabe der Absender-E-Mail-Adresse für die E-Mail-Benachrichtigungsvorlage verwendet; z.B. **noreply@localhost.com**.
E-Mail-Betreff	Geben Sie einen Betreff für die E-Mail-Vorlage ein. Er wird zur Definition des Betreffs der E-Mail-Benachrichtigungsvorlage verwendet; z.B. `<Hostname> - <Level> <Name>`.
E-Mail	Geben Sie Informationen für den Nachrichtentext der Vorlage ein, mit denen das Ereignis, der Ereigniszeitpunkt und der Schweregrad beschrieben werden.

5. Klicken Sie auf **Send Test Email** (Test-E-Mail senden), und prüfen Sie die Ergebnisse.
6. Wenn Sie mit den Ergebnissen des Tests zufrieden sind, klicken Sie auf **OK**.

Anpassen der Anzahl der Streams

Standardmäßig ist AppAssure so konfiguriert, dass drei gleichzeitige Streams auf das System zugelassen werden. Es wird empfohlen, dass die Anzahl der Streams um eins höher ist als die Anzahl der von Ihnen gesicherten Maschinen (Agenten). Wenn Sie z.B. sechs Agenten sichern, muss die **Maximale Anzahl gleichzeitiger Übertragungen** auf sieben eingestellt werden.

So ändern Sie die Anzahl der gleichzeitigen Streams:

1. Wählen Sie die Registerkarte **Konfiguration** aus und klicken Sie dann auf **Einstellungen**.
2. Wählen Sie in **Übertragungen-Warteschlange** „Ändern“ aus.
3. Ändern Sie die **Maximale Anzahl gleichzeitiger Übertragungen** auf eine Zahl, die mindestens um eins höher ist als die Anzahl der Clients, die Sie sichern.

Das Schützen von Maschinen und das Überprüfen der Client-Konnektivität

Überprüfen Sie nach dem Konfigurieren des DL Appliance und -Kerns, dass Sie sich mit den Maschinen verbinden können, die Sie sichern wollen.

So schützen Sie eine Maschine:

1. Wechseln Sie zur Kern-Konsole (Core Console) und wählen Sie die Registerkarte **Maschinen** aus.
2. Klicken Sie im Drop-Down-Menü **Maßnahmen** auf **Maschine schützen**.

   Das Dialogfeld **Verbinden** wird angezeigt.
3. Geben Sie die Informationen über die Maschine, mit der Sie Verbindung aufnehmen wollen, im Dialogfeld **Verbinden** ein, wie in der folgenden Tabelle beschrieben.

Host	Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten.
Schnittstelle	Die Portnummer, über die der AppAssure-Kern mit dem Agenten auf der Maschine kommuniziert.

Benutzername	Der Benutzername, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator.
Kennwort	Das Kennwort, das für die Verbindung mit dieser Maschine verwendet wird.

4. Klicken Sie auf **Verbinden**.
5. Wenn Sie eine Fehlermeldung erhalten, kann sich das Gerät nicht mit der Maschine verbinden, um diese zu sichern. So beheben Sie den Fehler:
   a. Überprüfen Sie die Netzwerkkonnektivität.
   b. Überprüfen Sie die Firewall-Einstellungen.
   c. Überprüfen Sie, ob die AppAssure-Dienste und RPC ausgeführt werden.
   d. Überprüfen Sie die DNS-Lookups (falls vorhanden)

Überprüfen der Netzwerk-Verbindungsfähigkeit

So überprüfen Sie die Netzwerkkonnektivität:

1. Öffnen Sie auf dem Client-System, mit dem Sie sich verbinden wollen eine Befehlszeilenschnittstelle.
2. Führen Sie den Befehl **ipconfig** aus und notieren Sie sich die IP-Adresse des Clients.
3. Öffnen Sie auf dem System eine Befehlszeilenschnittstelle.
4. Führen Sie den Befehl **ping <IP address of client>** aus.
5. Verfahren Sie je nach Ergebnis wie folgt:
   - Wenn der Client auf das Ping nicht antwortet, dann überprüfen Sie die Konnektivität des Servers und die Netzwerkeinstellungen.
   - Wenn der Client antwortet, dann überprüfen Sie, ob die Firewall-Einstellungen ein Ausführen der AppAssure-Komponenten zulassen.

Überprüfen der Firewall-Einstellungen

Wenn der Client ordnungsgemäß mit dem Netzwerk verbunden ist, jedoch durch die Kern-Konsole (Core Console) nicht erkannt wird, dann überprüfen Sie die Firewall, um sicherzugehen, dass eingehende und ausgehende Kommunikationen erlaubt sind.

So überprüfen Sie die Firewall-Einstellungen auf dem AppAssure-Kern und alle Clients, die dieser sichert:

1. Klicken Sie in der Appliance auf **Start** → **Systemsteuerung**.
2. Klicken Sie in der **Systemsteuerung** auf **System und Sicherheit**, und klicken Sie unter **Windows Firewall** auf **Firewall-Status überprüfen**.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Klicken Sie auf dem Bildschirm **Windows Firewall mit erweiterter Sicherheit** auf **Eingehende Regeln**.
5. Vergewissern Sie sich, dass für den AppAssure-Kern und die Ports in der Spalte **Aktiviert Ja** angezeigt wird.
6. Wenn die Regel nicht aktiviert ist, dann klicken Sie mit der rechten Maustaste auf den AppAssure-Kern und wählen Sie **Regel aktivieren** aus.
7. Klicken Sie auf **Ausgehende Regeln** und überprüfen Sie den AppAssure-Kern in gleicher Weise .

Überprüfen der Namensauflösung (falls vorhanden)

Wenn die Maschine, die Sie sichern wollen DNS verwendet, dann überprüfen Sie, ob Forward- und Reverse Lookups korrekt sind.

So stellen Sie sicher, dass die Reverse Lookups korrekt sind:

1. Gehen Sie im AppAssure-System in C:\Windows\system32\drivers\etc Hosts.
2. Geben Sie die IP-Adressen aller Kunden ein, die auf DL4300 sichern.

Teaming von Netzwerkkarten

Per Standardeinstellung sind die Netzwerkadapter (NICs) auf dem DL4300-Gerät nicht verbunden, was sich auf die Leistung des Systems auswirkt. Es wird empfohlen, dass Sie die NICs als einzelne Schnittstelle teamen. Für das Teaming der NICs ist Folgendes erforderlich:

- Neuinstallation der Broadcom Advanced Control Suite (Software-Suite für die erweiterte Broadcom-Konfiguration).
- Erstellung des NIC-Teams

Neuinstallation der Broadcom Advanced Configuration Suite (Software-Suite für die erweiterte Broadcom-Konfiguration)

So installieren Sie die Broadcom Advanced Configuration Suite erneut:

1. Gehen Sie zu C:\Install\BroadcomAdvanced und doppelklicken Sie auf Setup.
   Der, die, das InstallShield Wizard wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Ändern, Hinzufügen oder Entfernen**.
   Das Fenster **Benutzerdefiniertes Setup** wird angezeigt.
4. Klicken Sie auf **CIM-Anbieter** und wählen Sie anschließend **Diese Funktion wird auf der lokalen Festplatte installiert** aus.
5. Klicken Sie auf **BASP** und wählen Sie anschließend **Diese Funktion wird auf der lokalen Festplatte installiert** aus.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Installieren**.
8. Klicken Sie auf **Fertigstellen**.

Erstellung des NIC-Teams

ANMERKUNG: Es wird empfohlen, die native Teamschnittstelle in Windows 2012 Server **nicht** zu verwenden. Der Teaming-Algorithmus ist für ausgehenden und nicht für eingehenden Verkehr optimiert. Er bietet schlechte Leistung mit Sicherungsauslastung, sogar mit mehr Netzwerk-Ports im Team.

So erstellen Sie NIC-Teaming:

1. Wechseln Sie zu **Start → Search (Suche) → Broadcom Advanced Control Suite**

   ANMERKUNG: Bei dem Verwenden der Broadcom Advanced Control Suite wählen Sie nur die Broadcom Netzwerkkarten aus.

2. Wählen Sie in der **Broadcom Advanced Control Suite (Software-Suite für die erweiterte Broadcom-Konfiguration) Teams (Teams) → Go to Team View (Zu Team-Ansicht wechseln aus).**
3. Klicken Sie mit der rechten Maustaste links in den **Hosts lists** (Hosts-Listen) auf den Host-Namen des DL4300-Geräts, und wählen Sie **Create Team** (Team erstellen) aus.

   Das Fenster **Broadcom Teaming Wizard** (Broadcom Teaming-Assistent) wird angezeigt.
4. Klicken Sie auf **Next** (Weiter).
5. Geben Sie einen Namen für das Team ein und klicken Sie auf **Next** (Weiter).
6. Wählen Sie den **Team Type** (Team-Typ) aus und klicken Sie auf **Next** (Weiter).
7. Wählen Sie einen Adapter aus, den Sie zu einem Teil des Teams machen wollen und klicken Sie auf **Add** (Hinzufügen).
8. Wiederholen Sie diese Schritte für alle anderen Adapter, die Teil des Teams sind.
9. Wenn alle Adapter für das Team ausgewählt wurden, klicken Sie auf **Next** (Weiter).
10. Wählen Sie eine Standby-NIC aus, falls Sie eine NIC wollen, die als Standard-NIC verwendet wird, wenn das Team ausfällt.
11. Wählen Sie aus, ob **LiveLink** konfiguriert werden soll und klicken Sie anschließend auf **Next** (Weiter).
12. Wählen Sie **Skip Manage VLAN** (VLAN-Verwaltung überspringen) aus und klicken Sie auf **Next** (Weiter).
13. Wählen Sie **Commit changes to system** (Änderungen auf System anwenden) aus und klicken Sie auf **Finish** (Fertig stellen).
14. Klicken Sie auf **Yes** (Ja), wenn Sie gewarnt werden, dass die Netzwerkverbindung unterbrochen wurde.

    ANMERKUNG: Die Erstellung des Teams nimmt etwa 5 Minuten in Anspruch.

4

Installieren von Agenten auf Clients

Auf allen durch das AppAssure-System gesicherten Clients muss der AppAssure-Agent installiert sein. Mittels der Core Console (Kern-Konsole) können Sie Agenten auf Maschinen bereitstellen. Das Bereitstellen von Agenten auf Maschinen erfordert die Vorkonfiguration der Einstellungen zur Auswahl eines Agententypen, der auf die Clients (PUSH) aufgespielt werden soll. Diese Methode funktioniert, wenn auf allen Clients das gleiche Betriebssystem ausgeführt wird. Sind jedoch unterschiedliche Versionen von Betriebssystemen vorhanden, ist es für Sie möglicherweise einfacher, die Agenten auf den Maschinen zu installieren.

Sie können außerdem die Agentsoftware während des Schutzvorgangs der Maschine für die Agent-Maschine bereitstellen. Diese Option ist für Maschinen verfügbar, bei denen die Agentsoftware noch nicht installiert ist. Weitere Informationen zum Bereitstellen der Agentsoftware, während des Schutzes einer Maschine, siehe *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät) unter **dell.com/support/home**.

Remote-Installation von Agenten (Push)

So führen Sie eine Remote-Installation (Push) von Agenten durch:

1. Wenn der Client eine Betriebssystemversion ausführt, die älter ist als Windows Server 2012, dann überprüfen Sie, dass auf dem Client das Microsoft.NET4-Framework installiert ist:
   a. Starten Sie auf dem Client den **Windows Server-Manager**.
   b. Klicken Sie auf **Konfiguration → Dienste.**
   c. Stellen Sie sicher, dass in der Liste mit den Diensten das Microsoft .NET Framework angezeigt wird.

      Wenn es nicht installiert ist, können Sie für die Installation eine Kopie von **microsoft.com** beziehen.
2. Überprüfen und/oder ändern Sie den Pfad zu den Agenten-Installationspaketen:
   a. Klicken Sie in der AppAssure Core Console auf die Registerkarte **Konfiguration** und klicken Sie anschließend im linken Fensterbereich auf **Einstellungen**.
   b. Klicken Sie im Bereich **Einstellungen anwenden** auf **Ändern**.
   c. Vervollständigen Sie die folgenden Informationen zum Speicherort des Agenten:

Feld	Beschreibung
Agenten-Installationsprogrammname	Spezifiziert den exakten Pfad zum **folder\file** des Agenten.
Kern-Adresse	Spezifiziert die IP-Adresse des Systems, auf dem der AppAssure-Kern ausgeführt wird.

Feld	Beschreibung
	ANMERKUNG: Standardmäßig ist **Kern-Adresse** unausgefüllt. Das Feld **Kern-Adresse** benötigt keine IP-Adresse, da die Installationsdateien auf dem System installiert werden.

d. Klicken Sie auf **OK**.

3. Klicken Sie auf die Registerkarte **Extras** und klicken Sie anschließend im linken Fensterbereich auf **Massenbereitstellung**.

   ANMERKUNG: Sollte der Client bereits einen Agenten installiert haben, überprüft das Installationsprogramm die Version des Agenten. Ist der von Ihnen hinzugefügte Agent neuer als die installierte Version, bietet Ihnen das Installationsprogramm eine Aktualisierung des Agenten an. Sollte der Host die aktuelle Agentenversion installiert haben, stellt die Massenbereitstellung den Schutz zwischen dem AppAssure-Kern und dem Agenten her.

4. Wählen Sie in der Liste mit den Clients alle Clients aus und klicken Sie auf **Überprüfen**, um sicherzustellen, dass die Maschine aktiv ist und dass der Agent bereitgestellt werden kann.
5. Klicken Sie auf **Bereitstellen**, wenn in der Spalte **Meldung** bestätigt wird, dass die Maschine bereit ist.
6. Wählen Sie die Registerkarte **Ereignisse** aus, um den Status der Bereitstellung zu überprüfen.

   Nach Bereitstellen des Agenten wird automatisch mit einer Sicherung des Clients begonnen.

Bereitstellen der Agentensoftware beim Schutz eines Agenten

Sie können Agenten während des Vorgangs des Hinzufügens eines Agenten herunterladen und bereitstellen.

ANMERKUNG: Dieser Vorgang ist nicht erforderlich, wenn Sie bereits die Agent Software auf einer Maschine, die Sie schützen wollen, installiert haben.

Zum Bereitstellen der Agenten während des Vorgangs des Hinzufügens eines Agenten zum Schutz:

1. Klicken Sie von dem Dialogfeld **Protect Machine** (Maschine schützen) → **Connect** (Verbinden), nachdem Sie die entsprechenden Verbindungseinstellungen eingegeben haben, auf **Connect** (Verbinden).

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) wird angezeigt.
2. Klicken Sie auf **Yes** (Ja), um die Agent Software per Remote auf der Maschine bereitzustellen.

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) wird angezeigt.
3. Geben Sie die Anmelde- und Schutzeinstellungen, wie folgt ein:
   - **Host name** (Hostname) - Legt den Hostnamen oder die IP-Adresse der Maschine fest, die Sie schützen möchten.
   - **Port** (Port) - Legt die Portnummer fest, auf der der Kern mit dem Agenten auf der Maschine kommuniziert. Der Standardwert ist 8006.
   - **User name** (Benutzername) - Legt den Benutzernamen, der zum Verbinden der Maschine verwendet wird, fest; z. B. administrator.
   - **Passwort** (Kennwort) - Legt das Kennwort, das zur Verbindung dieser Maschine verwendet wird, fest.

- **Display Name** (Anzeigename) – Legt den Namen für die Maschine fest, die auf der Core Console angezeigt wird. Der Anzeigename kann der gleiche wie der Hostname sein.
- **Protect machine after install** (Maschine nach dem Installieren schützen) – Bei Auswahl dieser Option kann AppAssure, automatisch einen Basis-Snapshot erstellen, nachdem Sie die Maschine zum Schutz hinzugefügt haben. Diese Option ist per Standardeinstellung ausgewählt. Wenn Sie diese Option aufheben, müssen Sie manuell einen Snapshot erzwingen, wenn Sie bereit sind, den Datenschutz zu starten. Weitere Informationen über das manuelle Erzwingen eines Snapshots siehe „Forcing A Snapshot" (Erzwingen eines Snapshots) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät).
- **Repository** (Repository) - Wählen Sie das Repository aus, in welchem die Daten für diesen Agenten gespeichert werden sollen.

  ANMERKUNG: Sie können Daten von mehreren Agenten in einem einzelnen Repository speichern.
- **Encryption Key** (Verschlüsselungsschlüssel) - Bestimmt ob die Verschlüsselung auf die Daten für jedes in dem Repository gespeicherte Volumen auf dieser Maschine angewendet werden soll.

  ANMERKUNG: Sie können Verschlüsselungseinstellungen für ein Repository auf der Registerkarte **Configuration** (Konfiguration) in der Core Console definieren.

4. Klicken Sie auf **Deploy** (Bereitstellen).

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) wird geschlossen. Es kann zu einer Verzögerung kommen, bevor der ausgewählte Agent in der Liste der geschützten Maschinen aufgeführt wird.

Installieren von Microsoft Windows-Agenten auf dem Client

So installieren Sie die Agenten:

1. Überprüfen Sie, dass auf dem Client das Microsoft .NET4 Framework installiert ist:
   a. Starten Sie auf dem Client den **Windows Server-Manager**.
   b. Klicken Sie auf **Konfiguration → Dienste.**
   c. Stellen Sie sicher, dass in der Liste mit den Diensten das Microsoft .NET Framework angezeigt wird.

      Wenn es nicht installiert ist, können Sie eine Kopie von **microsoft.com** beziehen.
2. Installieren des Agenten:
   a. Geben Sie im AppAssure-System das Verzeichnis **C:\install\AppAssure** für den bzw. die Client(s) frei, den bzw. die Sie sichern wollen.
   b. Weisen Sie ein Laufwerk auf dem Client-System **C:\install\AppAssure** auf dem AppAssure-System zu.
   c. Öffnen Sie das Verzeichnis **C:\install\AppAssure** auf dem Client-System und doppelklicken Sie auf den für das System geeigneten Agenten, um mit der Installation zu beginnen.

Hinzufügen eines Agenten durch Verwenden des Lizenzportals

ANMERKUNG: Zum Herunterladen und Hinzufügen von Agenten müssen Sie Administratorrechte besitzen.

So fügen Sie einen Agenten hinzu:

1. Wählen Sie von der **Startseite des AppAssure-Lizenzportals** aus eine Gruppe aus und klicken Sie dann auf **Download Agent** (Agenten herunterladen).

   Es wird das Dialogfeld **Download Agent** (Agenten herunterladen) angezeigt.
2. Klicken Sie neben der Version des Installationsprogramms, die Sie herunterladen möchten, auf **Download** (Herunterladen).

   Folgende Optionen stehen zur Auswahl:

   - 32-Bit Windows-Installationsprogramm
   - 64-Bit Windows-Installationsprogramm
   - 32-Bit Red Hat Enterprise Linux 6.3, 6.4-Installationsprogramm
   - 64-Bit Red Hat Enterprise Linux 6,3, 6.4-Installationsprogramm
   - 32-Bit CentOS 6.3, 6.4-Installationsprogramm
   - 64-Bit CentOS 6,3, 6.4-Installationsprogramm
   - 32-Bit Ubuntu 12.04 LTS, 13.04-Installationsprogramm
   - 64-Bit Ubuntu 12.04 LTS, 13.04-Installationsprogramm
   - 32-Bit SUSE Linux Enterprise Server 11 SP2, SP3-Installationsprogramm
   - 64-Bit SUSE Linux Enterprise Server 11 SP2, SP3-Installationsprogramm
   - Microsoft Hyper-V Server 2012

   ANMERKUNG: Wir unterstützen diese Linux-Bereitstellungen und haben sie unter Verwendung der aktuellsten Kernel-Versionen getestet.

   ANMERKUNG: Agenten installiert auf Microsoft Hyper-V Server 2012 werden in dem Modus „Core Edition" von Windows Server 2012 betrieben.

   Die Datei mit dem **Agenten** wird heruntergeladen.
3. Klicken Sie im Dialogfeld des **Installationsprogramms** auf **Run** (Ausführen).

   ANMERKUNG: Weitere Informationen zum Hinzufügen von Agenten durch Verwendung der Core-Maschine siehe „Deploying An Agent (Push Install)" (Bereitstellen eines Agenten, Push-Installation) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät) unter **dell.com/support/home**.

Installieren von Agenten auf Linux-Maschinen

Laden Sie das verteilungsspezifische 32-Bit oder 64-Bit-Installationsprogramm auf alle Linux-Server herunter, die Sie unter Verwendung von AppAssure Core schützen wollen. Sie können die Installationsprogramme unter **https://licenseportal.com** vom AppAssure-Lizenzportal herunterladen. Beziehen Sie sich für weitere Informationen auf Hinzufügen eines Agenten durch Verwenden des Lizenzportals.

ANMERKUNG: Die Sicherheit beim Schutz einer Maschine basiert in Linux auf dem Pluggable Authentication Module (PAM). Nachdem ein Benutzer unter Verwendung von **libpam** authentifiziert wurde, ist der Benutzer nur dann zum Schutz der Maschine autorisiert, wenn er einer der folgenden Gruppen angehört:

- sudo
- admin
- appassure
- wheel

Weitere Informationen über den Schutz einer Maschine finden Sie im Abschnitt „Protecting a Machine" (Schutz einer Maschine) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät) unter **dell.com/support/home.**

Die Installationsanweisungen sind je nach der von Ihnen verwendeten Linux-Verteilung unterschiedlich. Beziehen Sie sich für weitere Informationen zum Installieren des Linux-Agenten auf Ihrer Verteilung auf folgendes:

- Installieren des Agenten auf Ubuntu
- Installation des Agenten auf Red Hat Enterprise Linux und CentOS
- Installieren des Agenten auf SUSE Linux Enterprise Server

ANMERKUNG: Wir unterstützen diese Linux-Bereitstellungen und haben sie unter Verwendung der aktuellsten Kernel-Versionen getestet.

ANMERKUNG: Die Installation des Linux Agent überschreibt alle Firewall-Regeln, die nicht durch UFW, Yast2 oder **system-config-firewall** angewandt wurden.

Wenn Sie manuell Firewall-Regeln hinzugefügt haben, müssen Sie die AppAssure-Ports nach der Installation manuell hinzufügen. Eine Sicherung der bestehenden Regeln wird unter **/var/lib/appassure/backup.fwl** geschrieben.

Sie müssen die Firewall-Ausnahmen auf allen Servern, die den AppAssure-Agenten zum Zugriff auf den Zugangsagenten für TCP-Ports 8006 und 8009 für AppAssure Core verwenden, hinzufügen.

Speicherort der Linux-Agenten-Dateien

Die Linux-Agenten-Dateien befinden sich bei allen Verteilungen in den folgenden Verzeichnissen:

Komponente	Speicherort/Pfad
mono	/opt/appassure/mono
Agent	/opt/appassure/aagent
aamount	/opt/appassure/amount
aavdisk and aavdctl	/usr/bin
configuration files for aavdisk	/etc/appassure/aavdisk.conf
wrappers for aamount and agent	• /usr/bin/aamount

Komponente	Speicherort/Pfad
	• /usr/bin/aagent
autorun scripts for aavdisk and agent	• /etc/init.d/appassure-agent • /etc/init.d/appassure-vdisk

Agenten-Abhängigkeiten

Die folgenden Abhängigkeiten werden benötigt und werden als Teil des Agenten-Installationsprogrammpakets installiert:

Für Ubuntu	Abhängigkeit
Das appassure-vss benötigt	`dkms, gcc, make, linux-headers-‘uname-r‘`
Das appassure-aavdisk benötigt	`libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3`
Das appassure-mono benötigt	`libc6 (>=2.7-18)`
Für Red Hat Enterprise Linux und CentOS	**Abhängigkeit**
Das nbd-dkms benötigt	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
Das appassure-vss benötigt	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
Das appassure-aavdisk benötigt	`nbd-dkms, libblkid, pam, pcre`
Das appassure-mono benötigt	`glibc >=2.11`
Für SUSE Linux Enterprise Server	**Abhängigkeit**
Das nbd-dkms benötigt	`dkms, gcc, make, kernel-syms`
Das appassure-vss benötigt	`dkms, kernel-syms, gcc, make`
Das appassure-aavdisk benötigt	`libblkid1, pam, pcre`
Das appassure-mono benötigt	`glibc >=2.11`

Installieren des Agenten auf Ubuntu

ANMERKUNG: Stellen Sie vor dem Durchführen dieser Schritte sicher, dass Sie das Ubuntu-spezifische Installationspaket in das Verzeichnis **/home/system** heruntergeladen haben.

Zum Installieren des AppAssure-Agenten auf Ubuntu:

1. Öffnen Sie eine Terminalsitzung mit Root-Zugriff.
2. Geben Sie den folgenden Befehl ein, um das AppAssure-Agenten-Installationsprogramm ausführbar zu machen:

   `chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

   Die Datei wird ausführbar gemacht.

   ANMERKUNG: Der Name des Installationsprogramms für 32-Bit-Umgebungen lautet **appassureinstaller_ ubuntu_i386_5.x.x.xxxxx.sh**
3. Geben Sie den folgenden Befehl ein, um den AppAssure-Agenten zu extrahieren und zu installieren:

   `/appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

   Der Linux-Agent beginnt mit dem Extrahieren und dem Installationsvorgang. Etwaige fehlende Pakete oder durch den Agenten benötigte Pakete oder Dateien werden heruntergeladen und automatisch als Teil des Scripts installiert.

   ANMERKUNG: Lesen Sie Agenten-Abhängigkeiten, um Informationen zu den durch den Agenten benötigten Dateien zu erhalten.

Nachdem das Installationsprogramm abgeschlossen wurde, wird der Agent auf der Maschine ausgeführt. Lesen Sie den Abschnitt „Protecting Workstations and Servers" (Schutz von Workstations und Servern) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Gerät) auf **dell.com/support/home**, um weitere Informationen über den Schutz dieser Maschine durch den Kern zu erhalten.

Installation des Agenten auf Red Hat Enterprise Linux und CentOS

ANMERKUNG: Stellen Sie vor dem Durchführen dieser Schritte sicher, dass Sie das Red Hat- bzw. CentOS-Installationspaket in das Verzeichnis **/home/system** heruntergeladen haben. Die folgenden Schritte sind für 32-Bit und 64-Bit-Umgebungen gleich.

Zur Installation des Agenten auf Red Hat Enterprise Linux und CentOS:

1. Öffnen Sie eine Terminalsitzung mit Root-Zugriff.
2. Geben Sie den folgenden Befehl ein, um das AppAssure-Agenten-Installationsprogramm ausführbar zu machen:

   `chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

   ANMERKUNG: Der Name des Installationsprogramms für 32-Bit-Umgebungen lautet `appassureinstaller__ rhel_i386_5.x.x.xxxxx.sh`.

   Die Datei wird ausführbar gemacht.

3. Geben Sie den folgenden Befehl ein, um den AppAssure-Agenten zu extrahieren und zu installieren:

   `/appassure-installer_rhel_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

   Der Linux-Agent beginnt mit dem Extrahieren und dem Installationsvorgang. Etwaige fehlende Pakete oder durch den Agenten benötigte Pakete oder Dateien werden heruntergeladen und automatisch als Teil des Scripts installiert.

   Lesen Sie Agenten-Abhängigkeiten, um Informationen zu den durch den Agenten benötigten Dateien zu erhalten.

Nachdem das Installationsprogramm abgeschlossen wurde, wird der Agent auf Ihrem Computer ausgeführt. Siehe Abschnitt „Protecting Workstations and Servers" (Schutz von Workstations und Servern) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät) auf **dell.com/support/home**, um weitere Informationen über den Schutz dieses Computers durch Core zu erhalten.

Installieren des Agenten auf SUSE Linux Enterprise Server

ANMERKUNG: Stellen Sie vor dem Durchführen dieser Schritte sicher, dass Sie das SUSE Linux Enterprise Server (SLES) Installationspaket in das Verzeichnis **/home/system** heruntergeladen haben. Die folgenden Schritte sind für 32-Bit und 64-Bit-Umgebungen gleich.

Zum Installieren des Agenten auf SLES:

1. Öffnen Sie eine Terminalsitzung mit Root-Zugriff.
2. Geben Sie den folgenden Befehl ein, um das AppAssure-Agenten-Installationsprogramm ausführbar zu machen:

   `chmod +x appassure-installer_sles_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

   ANMERKUNG: Der Name des Installationsprogramms für 32-Bit-Umgebungen lautet `appassureinstaller__ sles_i386_5.x.x.xxxxx.sh`

   Die Datei wird ausführbar gemacht.
3. Geben Sie den folgenden Befehl ein, um den AppAssure-Agenten zu extrahieren und zu installieren:

   `/appassure-installer_sles_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

   Der Linux-Agent beginnt mit dem Extrahieren und dem Installationsvorgang. Etwaige fehlende Pakete oder durch den Agenten benötigte Pakete oder Dateien werden heruntergeladen und automatisch als Teil des Scripts installiert.

   Lesen Sie Agenten-Abhängigkeiten, um Informationen zu den durch den Agenten benötigten Dateien zu erhalten.
4. Geben Sie bei Aufforderung zum Installieren der neuen Pakete `y` ein und drücken Sie anschließend <Eingabe>.

   Das System schließt den Installationsvorgang ab.

Nachdem das Installationsprogramm abgeschlossen wurde, wird der Agent auf Ihrer Maschine ausgeführt. Lesen Sie den Abschnitt „Protecting Workstations and Servers" (Schutz von Workstations und Servern) im *Dell DL4300 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4300-Gerät) auf **dell.com/support/home**, um weitere Informationen über den Schutz dieser Maschine durch Core zu erhalten.

5

Wie Sie Hilfe bekommen

Ausfindig machen der Dokumentation und Software-Aktualisierungen

In der AppAssure Core Console stehen direkte Links zu AppAssure, Gerätedokumentation und Softwareaktualisierungen zur Verfügung. Um auf die Links zuzugreifen, klicken Sie auf die Registerkarte **Appliance** (Gerät), und klicken Sie dann auf **Overall Status** (Allgemeinzustand). Sie finden die Links für die Softwareaktualisierungen und Dokumentation im Abschnitt **Documentation** (Dokumentation).

Softwareaktualisierungen

Direkte Links für AppAssure- und DL4300-Gerätesoftwareaktualisierungen sind von der AppAssure 5 Core Console erhältlich. Um auf die Links für Softwareaktualisierungen zuzugreifen, wählen Sie die Registerkarte **Appliance** (Gerät) aus, und klicken Sie dann auf **Overall Status** (Allgemeinzustand). Sie finden die Links für die Softwareaktualisierungen im Abschnitt **Documentation** (Dokumentation).

Kontaktaufnahme mit Dell

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

Dell bietet verschiedene online- und telefonisch basierte Support- und Serviceoptionen an. Wenn Sie über keine aktive Internetverbindung verfügen, so finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Dell Produktkatalog. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. Um sich bei Problemen zum Vertrieb, technischen Support oder zum Kundendienst mit Dell in Verbindung zu setzen, gehen Sie zu **software.dell.com/support**

Feedback zur Dokumentation

Klicken Sie auf allen Seiten der Dell Dokumentation auf den Link **Feedback**, füllen Sie das Formular aus und klicken Sie auf **Senden**, um uns Ihre Rückmeldung zukommen zu lassen.